ネットのリスク対策実践講座

巧妙化するネット犯罪 最新防衛策は、これだ!!

インターネットの常時接続、ホームページからの情報収集が当たり前の環境下では、ネット上のリスクを避けては通れない。しかも、ここ数年で脅威の質が劇的に変化しており、今やネット上で被る実害は金銭や信頼失墜にもつながりかねない状況だ。ここでは、ネットリスクの最新事情について解説した。一読後はぜひとも、会社や自宅でのセキュリティ対策の参考にしてほしい。

ここ最近のインターネットリスクは、犯罪色が一段と強まったことが大きな傾向だ。「金銭の搾取」を明確な狙いとした脅威がネット上に蔓延しており、被害は以前と比較にならないほど深刻化している。

その特徴は何といっても、プロ化が進み手口が複雑・巧妙化していること。一例を挙げると、07年夏頃から話題になり始めた「Mpack（エムパック）」（*1）だ。これは、マルウエア（*2）を遠隔地のパソコンへ強制的にインストールする不正プログラムである。

しかも、このMpackは取扱説明書が添付されて販売されているというから驚きだ。もちろん正規ルートで売られているわけではないが、意思さえあれば誰でも手に入れられることを意味する。

さらに、Mpackのような不正プログラムが他にも存在していることに加え、「こうした類のツールを自動的に仕掛けるプログラムさえも存在する」とセキュリティソフトメーカーの関係者。悪意を持つ犯罪者が、これらを利用して重要データなどを盗むことが容易となっているのだ。

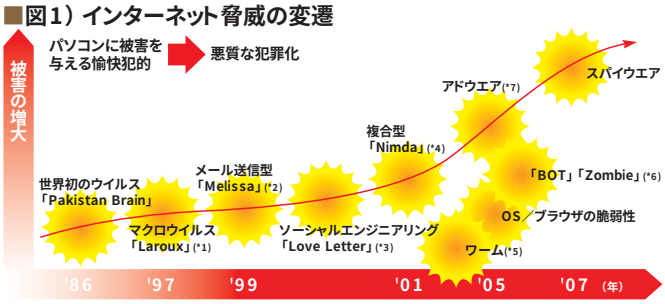
これだけではない。最近では個人のオンラインアカウントが不正に盗まれる被害（詳細は後述）が多発しており、このアカウントを売買する裏市場も存在しているという。

また、被害範囲も以前とは大きく様変わりしている。これまでの主流だったウイルスなどは、とにかく被害が広範囲にわたった。基本的に、ウイルスなど不正プログラムの開発には専門知識が必要となる。このため攻撃者が技術を誇示し自己顕示欲を満たしたいという思いから、「目立つこと」が大きな狙いだったからだ。

これに対して、ここ最近の傾向としては被害範囲が狭くなっていることが特徴といえる。というのも、攻撃者の目的が愉快犯的なものではなく明らかに犯罪化しているため、「とにかく目立たないこと」が重要となっているからだ。目立たなければ、セキュリティソフトメーカーなどに見つかりにくい。攻撃者が地域やターゲットを絞り込み犯罪実態や手口などの発覚を遅らせていることが、被害範囲の縮小につながっている。

こうした背景もあって、「ネットリスクは沈静化している」と安心しているユーザーも多いが、現実には決してネットからの脅威が軽くなっているわけではない。水面下に潜み悪質化したリスクにさらされている事実を肝に銘じることが必要だろう。

■図1）インターネット脅威の変遷



(*1) Laroux（ラルー）。マクロウイルスとは、「マクロ」と呼ばれる簡易プログラムの仕組みを悪用したウイルスで、ワープロ文書などに埋め込まれて実行される (*2) Melissa（メリッサ）。99年3月に猛威を振るったワーム型ウイルスで、電子メールを媒介に感染する (*3) Love Letter（ラブレター）。ソーシャルエンジニアリング（社会工学）を悪用したウイルス。ソーシャルエンジニアリングとは、人の心理に訴え、錯覚や誤解などにより相手から情報などを引き出すなど社会的手段を利用するテクニック。同ウイルスでは、「ラブレターを添付しました。読んでください」といったメッセージでウイルスが仕込まれた添付ファイルを開かせた (*4) Nimda（ニムダ）。01年9月にネット上で猛威を振るい、過去最悪といわれる被害を引き起こしたウイルス。複数のソフトウエアを介して、様々な手段で感染するという特徴を持った初の複合型ワームである。同種のもので、「CodeRed（コードレッド）」も同時期に流行した (*5) ワーム型ウイルスと呼ばれるウイルスの1種。他のプログラムに依存することなく、自己増殖を繰り返しながら破壊活動を行なう不正プログラム。作成が容易なため、亜種が多い (*6) BOT（ボット）／Zombie（ゾンビ）。いずれもユーザーが気付かないうちに、パソコンのリモートコントロールを可能にするスパイウエア系ウイルスである (*7) スパイウエアの1種。パソコン画面上に強制的に広告などをポップアップ表示させたり、HPの閲覧履歴などを収集するプログラム。本来は、企業などがユーザーの同意を得て利用する正規のプログラムだが、これが悪用されて詐欺などの手段として使われている

狙われている個人アカウント

では、具体的なリスクと実害はどうなっているのか。最近の傾向として、特に注意したいのは①個人情報（オンラインアカウント）の搾取、②オンライン詐欺、③情報漏えい――この3つだ。詳細を見ていこう。

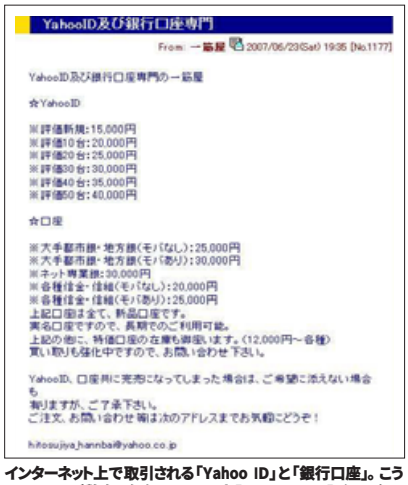
最近、特に急増しているのが①個人情報の搾取である。ここでいう個

人情報とは、ネット上で利用しているIDやパスワードなどのオンラインアカウントのこと。インターネットバンキングやクレジットカードなどの個人ページ、「Yahoo！」に代表されるポータルサイトやSNS、オークション用など様々なアカウントをネット上で使っているはずだ。犯罪者は、こうした個人アカウントを盗み出して悪用している。

オンラインアカウントが盗用された場合、実害としては「直接的な金銭被害」と「間接的な被害」という2つの側面がある。前者は文字通り金銭的な損失を意味しており、インターネットの銀行口座やクレジットカードの番号などが盗用され、預金の不正引き出しやカードの不正利用により現実的な被害が発生する。

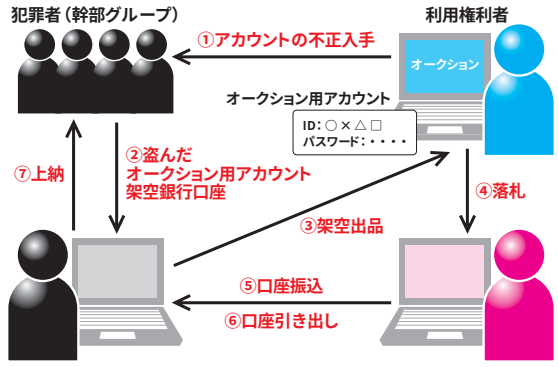
最近はインターネット銀行やクレジットカードの手続き、融資依頼などをホームページ（以下HP）上で行なうケースも増えている。HPへのアクセス用アカウントが盗まれて、被害にあうケースも増えているのだ。

実際、預金などが不正引き出されたという事例が急増。例えば全国銀行協会実施のアンケート（*3）によると、ネット上で預金が不正に引き出されたとの報告は06年までは四半期ベースで十数件レベルだった。ところが、07年以降は30～50件を超える被害が発生。07年9月末時点までの累計で報告件数128件、被害額1億2300万円とすでに前年の約3倍にも達している。



インターネット上で取引される「Yahoo ID」と「銀行口座」。こうしたサイトが数多く存在している。上記サイトでは、評価50台のYahoo IDが4万円で販売されていた

■図2）オンラインアカウントを悪用したオークション詐欺



※実際に日本国内で検挙された事例（資料提供：ウエブルート・ソフトウエア）

一方、「間接的な被害」とは、金銭は絡まないが信用失墜などにつながりかねないもの。オークションIDやSNS、無料のウエブメールなどのアカウントが悪用されることが原因だ。

最も分かりやすい例は、オークションIDが詐欺に悪用されるケースだろう（図2）。不正入手したオークション用のアカウントを使い高額商品などを架空出品し、代金だけを落札者からだまし取るのである。オークションID以外にも様々なオンラインアカウントが、こうした詐欺などの踏み台として悪用されている。当然、被害届が出されれば最初に疑われるのはアカウント本来の所有者であり、無実が分かったとしても信用問題につながることは避けられない。

これらのオンラインアカウントは銀行やクレジットカードに比べて、ユーザーにとって重要度が低い。管理も甘く、犯罪者にとっては、それだけリスクが低いということだ。

発覚するリスクが低いにも関わらず、詐欺ツールなどとして利用価値は大きい。しかも、オンラインアカウントそのものがネット上で取引されているほど。例えば、オークションIDなどは評価数（*4）により取引額が決まる。基本的に評価数が多いほど入札者の信頼性も高く、1000を超える評価が書き込まれたIDは10万円以上で取引されているという。

正規ＨＰも改ざんの危険性

個人アカウントは、「スパイウエア」や「フィッシング（Phishing）」などの方法で搾取されている。

特に巧妙化しているのが、「スパイウエア（*5）」の手口である。スパイウエアとは、パソコン内に侵入してユーザーが意図しない動作を勝手に行なう不正プログラムのこと。アカウントを搾取するようプログラムされたスパイウエアが知らないうちにインストールされ、個人アカウントが盗まれているのだ。

スパイウエアが送り込まれるルートは様々で、以前に比べてかなり高度化しているだけにやっかいだ。これまではスパムメール（迷惑メール）、アダルトやアンダーグラウンドサイトなどいかがわしいHP経由で侵入するルートがほとんどだった。だが、企業など正規のHPが改ざんされ、そこからスパイウエアを送り込まれるケースが最近は相次いでいる。

その手口はこうだ。改ざんされた企業などのHPにアクセスすると、意図せずに当該企業とは別のHP（罠サイト）が表示される。罠サイトにはスパイウエアが仕掛けられており、そこからアカウントを盗む不正プログラムがインストールされるのだ。

こうしたHPがネット上に数万サイトも見つかったとの報告さえある。というのも、この仕掛け作りがいたって簡単なことが大きな理由だろう。

詳細は省くが、HP上で別ウインドウを自由に開く技術「iFrame（アイフレーム）」と呼ばれるコードを利用

して罠サイトへと誘引する。正規HPにコードを仕掛けるには知識や技術が必要だが、様々な不正ツールの入手が可能なため、知識のない悪意の犯罪者でも容易に罠を仕掛けられる。こうした背景から、個人アカウントの搾取が急増しているのだ。

また、偽装HPによりユーザーからアカウントなどをだまし取る「フィッシング（*6）」被害も減る気配を見せない。それどころか、正規HPと見分けがつかないほど精巧に作成されるなど、ますます巧妙化している。

セキュリティソフトを使った詐欺的アプリケーションの例。HPを閲覧中に上記のようなウインドウが開き、パソコンが脅威にされされていると警告してくる。ネットリスクに対する不安を煽った、一種のソーシャルエンジニアリングを利用した手口ともいえる。ほとんどはフラッシュ技術で作成されたもの。続いて、脅威を取り除くためにセキュリティソフトを購入するよう促してくるが、中にはダウンロード後になって初めて代金を請求するものもあるようだ。右画面は支払データの入力を求めているもの。迂闊に入力してしまえば、何に悪用されるか分からない

詐欺的アプリケーションの広告。製品名は「Virus Wadame」だが、全く同じ製品パッケージとテキストで「Virus Seigyo」「Virus VanGuard」「ベスト保護」といった商品も見つかった。最大の対策は、「信用できるメーカーや販売サイト以外からは商品を購入しないこと」だ

典型的なクリック詐欺の請求画面。契約確認画面でのキャンセル可能な仕組みや契約成立メールの送信など電子消費者契約法に基づく契約成立要件を満たしていない。基本的には、ひたすら無視すること。頻繁にこのウィンドウがポップアップ表示されたり、メールを送り付けられたりすることもあるが、絶対に問い合わせてはいけない。相手は詐欺師、思う壺である

従来リスクも複雑・巧妙化

②オンライン詐欺では、「詐欺的アプリケーション」や「ワンクリック詐欺」などの勢いが衰えない。いずれもユーザー心理を巧みについて、金銭をだまし取る手法である。

詐欺的アプリケーションとは、役に立たないソフトなどを購入させて代金を払わせようとする手法で、セキュリティ不安を揺さぶるタイプが有名だ。HPを閲覧中に突然、ウイルス感染やシステムエラーなどを警告するメッセージが表示され、対策ソフトをダウンロードするよう促してくる。指示通りにソフトをインストールすると、購入料金が請求される。

警告はフラッシュ（*7）で作成された偽装メッセージで、実際には何の被害も発生していない。ダウンロードしたソフトも、多くは役に立たないことが多いという。

米国などで先行した被害が国内へ流れ込んできたのだが、今は明らかに日本人を狙ってきている。以前は妙な日本語が多く詐欺であることを見抜くのは容易だったが、最近はこなれた日本語を使うケースも見られるようになり油断ならない状況だ。

「ワンクリック詐欺」は説明するまでもないだろう。閲覧承諾表示やHPアドレスなどをクリックすると、契約が発生したように見せかけて利用料をだまし取る手口である。これを少し巧妙化させたのが、「ツークリック詐欺」。ワンクリック後に契約の同意を得るためのメッセージを小さく表記することで、電子消費者契約法に基づく請求のように見せかける。

こうした基本的な手口は、最近も変わらない。やっかいな点は絶えず請求画面がポップアップ表示されたり、請求メールが毎日送られてくるケースがあること。請求画面が常時ポップアップされるのはスパイウエアのインストールが考えられ、請求メールはクリックした際にアドレス情報が搾取されたことが原因だ。

特に、請求メールが数時間ごとに送信されてくるとセキュリティ知識を持つユーザーでも心理的に不安になる。小額訴訟など法律用語を駆使してくるため、「自分の知らない法律があるのでは」といった不安から連絡したり、料金を振り込んでしまうユーザーが少なくないという。よく見れば不可解な内容が必ずあるのだが、冷静さを失うと見逃してしまいがちなことから被害が後を絶たない。

さらには、ネット上からの③情報漏えいの危険性も相変わらずだ。ファイル共有ソフト「Winny（ウィニー）」を温床とした漏えい問題はあまりにも有名。同ソフトの使用を禁止する企業などが続出した。

それでもネット上で情報漏えいしたとの話が漏れ聞こえてくる。そもそもパソコンからネット上に情報が流出する原因は「情報暴露型ウイルス」に感染したこと。ウィニーは感染率が高いとうだけで、ソフト自体に問題があるわけではない。ファイル共有ソフトは、匿名性が高く一次配布者を特定しにくいことから、ウイルスを仕掛ける絶好の場なのだ。

「Share（シェア）」や「Lime Wire（ライム・ワイヤー）」などウィニー以外にもファイル共有ソフトが存在し、これらを使う限り感染リスクからは免れないだろう。

①～③で挙げた以外にも、05年から猛威を振るっている「BOT（*8）」や一時期になりを潜めていた「ランサムウエア（*9）」が復活するなど、

ネット上には新旧入り混じった様々な不正プログラムが存在している。リスクの犯罪化と相まって、ネットの脅威は高まっているのだ。

ソフト導入前提に人的対策

では、こうした脅威にはどう対応していけばいいのだろうか。結論からいうと、まず「セキュリティソフトを必ず導入」し、その上で「人的／組織的な対策を講じていくこと」だ。

プロ集団により複雑かつ巧妙化されたリスクを、人的対応だけで防ぐことは難しい。正規のHPでさえ改ざんされる可能性がある状況では、「信頼できないHPは閲覧しない」といった従来の人的な考え方だけでは限界がある。セキュリティ対策ソフトの導入は不可欠といえるだろう。

この基本的な考え方をベースに、具体的には「セキュリティソフトの確実な導入と稼動」「OSやインターネットブラウザの更新」「組織的／人的な対策」という3方向からリスクに備えることが大きなポイントだ。

まず、「セキュリティソフトの確実な導入と稼動」として、ウイルスからスパイウエアまで幅広く対応可能な総合セキュリティソフトの導入を勧めたい。というのも、感染力を持つマルウエアなどウイルスとスパイウエアの特徴を併せ持つ種類が増え手口も巧妙化していることから、従来のように個別ソフトでは被害を防ぎ切れなくなってきたからである。

セキュリティソフトを、すべてのパソコンに導入することも不可欠だ。メイン機にはインストールしていながら、サブ機は無防備というケースが意外と多いもの。ネットワークに接続する以上は、どこでリスクにさらされるか分からないと肝に銘じたい。

また、セキュリティソフトを導入していながら、稼動させていないケースが驚くほど多い。スキャン動作がメモリとCPUをかなり占有するため、時としてパソコンが重くなり使い勝手が悪くなる。これを避けようと、セキュリティソフトを切ってしまうことが理由だ。ネットリスクの最新事情を知った以上、オフにするようなことはできないはずである。

「OSやインターネットブラウザの更新」も欠かせない対策だ。ウイルスやスパイウエア、不正アクセスなどは侵入ルートとしてセキュリティホール（セキュリティ上の欠陥）を狙ってくる。この欠陥を修正するためのプログラムが配布されるので、必ず更新することが重要となる。

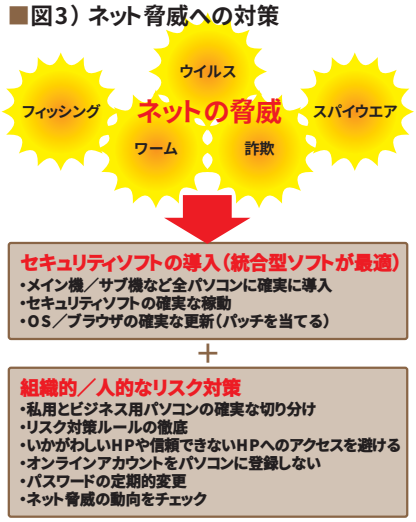
前出のMpackはブラウザの脆弱性を狙って強制インストールを仕掛けてくるため、ブラウザの更新により被害を防ぐことができる。

現在のインターネット社会では、こうした物的措置を講じることで初めて、「組織的／人的な対策」が生きてくる。組織としては、やはり情報漏えいが最大の懸念事項だろう。原因となる情報暴露型ウイルスの感染を防ぐには、危険性の高いファイル共有ソフトなどの使用禁止が欠かせない。このためにも、パソコンの私的利用と業務利用を確実に切り分けることが重要なポイントとなる。

特に、メインやサブ機も含めパソコンの使用を社員所有のものに頼っている企業は注意が必要だ。万全を期すには、やはり会社側から支給すると共にリスク管理のルール徹底が不可欠だろう。

人的対策としては、「信頼できないHPは閲覧しない」「個人情報の入力には細心の注意を払う」といった基本的な方法で念を入れたい。アカウントを打ち込む必要がある場合、当該HPのSSL（*10）対応やブラウザの画面右下に表示される鍵マークをクリックして「サーバー証明書」をチェックするといった対策は現在も有効である（弊誌18号に詳述）。

■図3）ネット脅威への対策



アカウントを、しっかりと管理することも重要。面倒だからと、IDやパスワードをパソコンに記録して入力の手間を省いているユーザーも多いが、できれば避けたい。万一、スパイウエアの侵入を許した場合、根こそぎ情報を搾取されるからだ。また、パスワードを定期的に変更するなど地道な対策も必要だろう

ネットの脅威に対し、もはやセキュリティソフトが不可欠だ。加えて、セキュリティ動向を少しでもチェックし、知識を身につけておくことが脅威から身を守ることにつながる。

(*1)「Dream Coders Team」と自称する関係者により開発された不正プログラム。取扱説明書で使用されている言語からロシア発祥と見られている。開発者により日々バージョンアップされているという
(*2)ウイルスやワーム、スパイウエアの中でも悪意を持つリスクの総称
(*3)同協会の正会員と準会員184行を対象として実施
(*4)オークションの取引ごとに書き込まれる評価のことで、入札や落札の参考にされる指標となる
(*5)特に犯罪行為を目的とした悪質なものは「クライムウエア」と呼ばれており、キー入力を外部から読み取る「キーロガー」やウイルスとスパイウエアの特徴を兼ね備える「トロイの木馬」などがある
(*6)銀行やクレジットカード会社などの実在企業の偽HPを作成。当該企業を装って電子メールなどにより偽サイトへ誘導し、口座やカード番号、IDやパスワードなどを入力させて個人情報を不正に搾取する手口
(*7)HP上でイラストやアニメーションを動かしたり、効果音を出せるソフトウエア
(*8)ウイルス系不正プログラム。スパイウエア的に機能するが、感染力があるためウイルスとして定義されている。感染したパソコンはネットワーク経由で遠隔コントロールされ、犯罪の踏み台として利用されてしまう
(*9)パソコン内の情報やデータを暗号化してしまい、複合の条件として金銭や商品購入などを要求してくる不正プログラム。データを人質にとって金銭を奪うことから、英語で身代金を意味する「ランサムウエア」と呼ばれている
(*10)インターネット上でやり取りするデータを暗号化し、個人情報や重要事項などを安全に送受信するための規格